Implementing Cisco Edge Network Security Solutions (SENSS)

ID: CI-SENSS  Price: £2,732.- (excl. VAT)  Duration: 5 days

Course Overview
Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 is a newly created five-day instructor-led training (ILT) course, which is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP® Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience to prepare them to configure Cisco perimeter edge security solutions utilizing Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls. The goal of the course is to provide you with foundational knowledge and the capabilities to implement and managed security on Cisco ASA firewalls, Cisco Routers with the firewall feature set, and Cisco Switches. You will gain hands-on experience with configuring various perimeter security solutions for mitigating outside threats and securing network zones. At the end of the course, you will be able to reduce the risk to their IT infrastructures and applications using Cisco Switches, Cisco ASA, and Router security appliance feature and provide detailed operations support for these products.

Who should attend
The primary audience for this course is as follows:

- Network Security Engineers

Prerequisites
This section lists the skills and knowledge you must possess to benefit fully from the course. This section includes recommended Cisco learning offerings that you may complete to benefit fully from this course, including the following:

- Cisco Certified Network Associate (CCNA®) certification
- Cisco Certified Network Associate (CCNA®) Security certification
- Knowledge of Microsoft Windows operating system

Course Objectives
Upon completing this course, you will be able to meet these overall objectives:

- Understand current security threat landscape
- Understanding and implementing Cisco modular Network Security Architectures such as SecureX and TrustSec
- Deploy Cisco Infrastructure management and control plane security controls
- Configuring Cisco layer 2 and layer 3 data plane security controls
- Implement and maintain Cisco ASA Network Address Translations (NAT)
- Implement and maintain Cisco IOS Software Network Address Translations (NAT)
- Designing and deploying Cisco Threat Defense solutions on a Cisco ASA utilizing access policy and application and identity based inspection
- Implementing Botnet Traffic Filters
- Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW)
- Configure and verify Cisco IOS ZBFW Application Inspection Policy

Detailed Course Outline

Module 1: Secure Design Principles

- Course Overview
- Network Security Zoning
- Cisco Module Network Security Architecture
- Cisco SecureX Architecture and Cisco TrustSec Solution

Module 2: Deploying Network Infrastructure Protection

- Intro Cisco Network Infrastructure Architecture and Deploying Cisco IOS Control Plane Security Controls, Cisco IOS Management Plane Security Controls
- Deploying Cisco ASA Management Plane Security Controls
- Lab 2-1: Configuring Control and Management Plane Security
• Configuring Cisco Traffic Telemetry Methods
• Lab 2-2: Configuring Cisco Traffic Telemetry Methods
• Deploying Cisco IOS Layer 2 and Layer 3 Data Plane Security Controls
• Lab 2-3 and 2-4: Configuring Cisco Layer 2 and Layer 3 Data Plane Security

Module 3: Deploying NAT on Cisco IOS and Cisco ASA

• Introducing Network Address Translation
• Deploying Cisco ASA Network Address Translation
• Lab 3-1: Configuring Cisco ASA NAT
• Deploying Cisco IOS Software Network Address Translation

Module 4: Deploying Threat Controls on Cisco ASA

• Introducing Cisco Threat Controls
• Deploying Cisco ASA Basic Access Policies
• Lab 4-1: Configuring Cisco ASA Access Policy
• Deploying Cisco ASA Application Inspection Policies
• Lab 4-2: Configuring Authentication Using WebAuth
• Deploying Cisco ASA Botnet Traffic Filtering
• Lab 4-3: Configuring Cisco ASA Botnet Traffic Filter
• Deploying Cisco ASA Identity Based Firewall
• Lab 4-4: Configuring Cisco ASA Identity Based Firewall

Module 5: Deploying Threat Controls on Cisco IOS Software

• Deploying Cisco IOS Software with Basic Zone-Based Firewall Policy
• Lab 5-1: Configure Cisco IOS Software with Basic ZBFW
• Deploying Cisco IOS Software ZBFW with Application Inspection Policies
• Lab 5-2: Configure Cisco IOS Software ZBFW with Application Inspection Policy